UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/988,300	11/19/2001	Adrian Walker		8404

7590 09/27/2005

ADRIAN WALKER
REENGINEERING LLC
PO Box 1412
BRISTOL, CT 06011

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 09/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/988,300	WALKER, ADRIAN	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 November 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-34 are pending and have been examined.

Information Disclosure Statement

2. The listing of references in the specification is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, or other information submitted for consideration by the Office, and MPEP § 609.04(a) states, "the list may not be incorporated into the specification but must be submitted in a separate paper." Therefore, unless the references have been cited by the examiner on form PTO-892, they have not been considered.

Drawings

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 118 (fig 1). Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

4. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code (page 3, lines 3, 6). Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Claim Objections

5. Claim 1 is objected to because of the following informalities: "a computer-implemented method and system". All the dependent claims are drawn on a method. Claim 1 has been interpreted as reciting ""a computer-implemented method" for the purposes of this document. Furthermore, even though claim 1 attempts to recite a method, the language does not specifically recites any steps, but describes what an attacker does or may do. Appropriate correction is required.

6. Claims 14-16 are objected to because of the following informalities: "in which in which". Perhaps just one "in which" was intended. Appropriate correction is required.

7. Claim 22 and 25 are objected to because of the following informalities: "containing copies of **symbols in the that occur in** plaintext" (emphasis added). Appropriate correction is required.

8. Claim 32 is objected to because of the following informalities: "sytematically". Perhaps "systematically" was intended. Appropriate correction is required.

9. Claims 33 and 34 are objected to because of the following informalities: "for for". Perhaps just one "for" was intended. Appropriate correction is required.

Claim Rejections - 35 USC § 112

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The terms "reasonably" and "reasonable" in claim 1 are relative terms which render the claim indefinite. The terms "reasonably" and "reasonable" are not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. "**Reasonably** select and arrange some of the symbols to produce a **very large number** of decrypt attempts".

12. Claim 1 is rejected as failing to define the invention in the manner required by 35 U.S.C. 112, second paragraph.

The claim(s) are narrative in form and replete with indefinite and functional or operational language. The structure which goes to make up the device must be clearly and positively specified. The structure must be organized and correlated in such a manner as to present a complete operative device. The claim(s) must be in one sentence form only. Note the format of the claims in the patent(s) cited.

Claim Rejections - 35 USC § 102

13. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

14. Claims 33-34 are rejected under 35 U.S.C. 102(b) as being anticipated by Hartman, Jr. (US Patent Number 5,500,897, hereinafter "Hartman").

Regarding claim 33, Hartman teaches an apparatus for encryption and decryption of text audio, graphic, video or other data (column 1, lines 14-35), comprising at least one computer (column 4, lines 25-57).

Regarding claim 34, Hartman teaches an apparatus for encryption and decryption of text audio, graphic, video or other data (column 1, lines 14-35), comprising two or more computers connected over at least one network (column 4, lines 25-57).

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. Claims 1-13 and 28-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman, and further in view of Litwin, Jr. et al. (US Patent Number 6,703,923, hereinafter "Litwin").

Regarding claim 1, Hartman teaches a computer-implemented method and system for encryption and decryption of text audio, graphic, video or other data. Hartman does not expressly disclose that an attacker who seeks to recover a plaintext from a ciphertext, can reasonably select and arrange some of the symbols of the ciphertext to produce a very large number of decrypt attempts that are plausible, but that are unrelated in meaning to the original plaintext; and an attacker who seeks to recover a plaintext from a ciphertext, who does not know the specific key used for encryption, cannot know whether any one of a number of attempted decrypts he produces, by means of a reasonable selection and arrangement of some of the symbols of the ciphertext, is a correct original plaintext. However, Litwin teaches comprising steps such that: an attacker who seeks to recover a plaintext from a ciphertext, who may or may not know the general encryption method, but who does not know the specific key used for encryption, can reasonably select and arrange some of the

symbols of the ciphertext to produce a very large number of decrypt attempts that are plausible, but that are unrelated in meaning to the original plaintext; and an attacker who seeks to recover a plaintext from a ciphertext, who may or may not know the general encryption method, but who does not know the specific key used for encryption, cannot know whether any one of a number of attempted decrypts he produces, by means of a reasonable selection and arrangement of some of the symbols of the ciphertext, is a correct original plaintext (column 2, lines 35-60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Hartman and Litwin. One of ordinary skill in the art would have been motivated to do so to encrypt information transfers (Litwin, column 1, lines 30-67).

Regarding claim 2, the combination of Hartman and Litwin teaches the limitations as set forth under claim 1 above. Furthermore, Litwin teaches that if the same plaintext is encrypted twice using the same key, the respective ciphertexts may be different (column 2, lines 35-60).

Regarding claim 3, the combination of Hartman and Litwin teaches the limitations as set forth under claim 1 above. Furthermore, Litwin teaches that if the same plaintext is encrypted twice using the same key, the respective ciphertexts may have different lengths (column 2, lines 35-60).

Regarding claim 4, the combination of Hartman and Litwin does not expressly disclose comprising steps in which a key for encryption and decryption contains a named integer. However, Examiner takes Official Notice that using integers as keys for

encryption/decryption was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use integers as keys for encryption/decryption since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 5, the combination of Hartman and Litwin does not expressly disclose further comprising steps in which a key for encryption and decryption contains a named set of symbols. However, Examiner takes Official Notice that using a named set of symbols as keys for encryption/decryption (Navajo code talkers used their native tongue to securely communicate messages for the military during World War II, a named set of symbols) was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a named set of symbols for encryption/decryption since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 6, the combination of Hartman and Litwin teaches the limitations as set forth under claim 1 above. Furthermore, Hartman teaches further comprising steps in which a key for encryption and decryption contains an executable computer program (column 4, lines 24-67).

Regarding claim 7, the combination of Hartman and Litwin teaches the limitations as set forth under claim 6 above. Furthermore, Hartman teaches further comprising steps in which a key for encryption and decryption contains an executable computer program, in object code form, that is made known to an encryption program at

run time, and that is made known to a decryption program at run time (column 4, lines 24-67).

Regarding claim 8, the combination of Hartman and Litwin teaches the limitations as set forth under claim 6 above. Furthermore, Hartman teaches further comprising steps in which a key for encryption and decryption contains an executable computer program that generates and uses pseudo random numbers (column 2, lines 28-43).

Regarding claim 9, the combination of Hartman and Litwin does not expressly disclose using of a source of genuinely random numbers. However, Examiner takes Official Notice that the use of a source of genuinely random numbers for encryption purposes was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use of a source of genuinely random numbers for encryption purposes since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 10, the combination of Hartman and Litwin does not expressly disclose further comprising steps in which a key contains a table describing an encoding of a digit in the range 0-9 into two or more choices of symbols, such that a symbol amongst the choices for a given digit does not occur amongst the choices for any other digit. However, Examiner takes Official Notice that encoding (assigning an arbitrary meaning to a symbol) was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have a table describing an encoding of a digit in the range 0-9 into two or more choices

of symbols since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 11, the combination of Hartman and Litwin does not expressly disclose generating a permutation of the numbers 1, . . . ,n, where n is given as input to the generator. However, Examiner takes Official Notice that the use of a source of genuinely random numbers or a pseudo random number generator, generating a permutation of the numbers 1, . . . ,n, where n is given as input to the generator, for encryption purposes was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a permutation of the numbers 1, . . . ,n, where n is given as input to the generator since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 12, the combination of Hartman and Litwin does not expressly disclose the generator generates only a permutation that does not contain any sequential subsequence of a specified length. However, Examiner takes Official Notice that generating only a permutation that does not contain any sequential subsequence of a specified length was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate only a permutation that does not contain any sequential subsequence of a specified length since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 13, the combination of Hartman and Litwin teaches the limitations as set forth under claim 1 above. Furthermore, Hartman teaches further

comprising steps in which a key contains a function depending on the length of a plaintext to be encrypted or decrypted, depending also on a named integer that is part of the key, and depending also on a pseudo random or genuinely random integer, the function producing a sequence of apparently random integers in a prescribed range (column 4, lines 24-67).

Regarding claim 28, the combination of Hartman and Litwin teaches the limitations as set forth under claim 1 above. Furthermore, Hartman teaches a processor for encryption/decryption. Applicant also admits the use of padding was known (page 1). Furthermore, Examiner takes Official Notice that decrypting using a function (to decipher an encoded message) and using padding was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to decrypt using a function and separate the padding information, this information containing information about how the ciphertext was created since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 29, the combination of Hartman and Litwin teaches the limitations as set forth under claim 1 above. Furthermore, Hartman teaches a processor for encryption/decryption. Applicant also admits the use of padding was known (page 1). Furthermore, Examiner takes Official Notice that decrypting using a function (to decipher an encoded message) and using padding was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to decrypt using a function and separate the padding

information since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 30, the combination of Hartman and Litwin teaches the limitations as set forth under claim 1 above. Furthermore, Hartman teaches a processor for encryption/decryption. Applicant also admits the use of padding was known (page 1). Furthermore, Examiner takes Official Notice that decrypting using a function (to decipher an encoded message) and using padding was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to decrypt using a function and separate the padding information since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 31, the combination of Hartman and Litwin does not expressly disclose in which a key contains a function that a decrypter may use to apply an inverse permutation to a permuted sequence of plaintext symbols in order to recover an original sequence of plaintext symbols. However, Examiner takes Official Notice that decrypting using a function (to decipher an encoded message) was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to decrypt using a function since Examiner takes Official Notice that it was conventional and well known.

17. Claims 14-17 and 20-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman and Litwin, and further in view of Menezes et al. (NPL document "Handbook of Applied Cryptography", hereinafter "Menezes").

Regarding claim 14, the combination of Hartman and Litwin does not expressly disclose steps in which a key contains a program capable of encoding a number, digit-by-digit, into a sequence of symbols, using a pseudo random number generator, or using a source of genuinely random numbers, the pseudo random or genuinely random numbers being used to choose amongst the choices in a table for the encoding of each digit. However, Menezes teaches steps in which a key contains a program capable of encoding a number, digit-by-digit, into a sequence of symbols, using a pseudo random number generator, or using a source of genuinely random numbers, the pseudo random or genuinely random numbers being used to choose amongst the choices in a table for the encoding of each digit (pages 224-251, 420-424). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to randomly choose the order of encryption. One of ordinary skill in the art would have been motivated to do so because it was well known to randomly choose the order of encryption (Menezes, pages 224-251, 420-424).

Regarding claim 15, the combination of Hartman, Litwin, and Menezes teaches the limitations as set forth under claim 14 above. Furthermore, Menezes teaches steps in which a sequence encoding a positive number, is padded, digit-by-digit, with additional symbols not among the choices in a table, but including symbols from an input plaintext, using a pseudo random number generator, or using a source of genuinely random numbers, to choose the padding symbols (pages 224-251, 420-424).

Regarding claim 16, the combination of Hartman, Litwin, and Menezes teaches the limitations as set forth under claim 15 above. Furthermore, Menezes teaches steps

in which in which a padded sequence that encodes a positive number, is decoded digit-by-digit, using a table, ignoring padding symbols not among the choices in the table, to obtain the unencoded number (pages 224-251, 420-424).

Regarding claim 17, the combination of Hartman and Litwin does not expressly disclose steps in which a key contains a function with one input integer, that produces as output an integer in the range between 0 and the input, that output being used as the start position in which a sequence of padded encoded information is inserted into a ciphertext. However, Menezes teaches steps in which a key contains a function with one input integer, that produces as output an integer in the range between 0 and the input, that output being used as the start position in which a sequence of padded encoded information is inserted into a ciphertext (pages 224-251, 420-424). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to randomly choose the order of encryption. One of ordinary skill in the art would have been motivated to do so because it was well known to randomly choose the order of encryption (Menezes, pages 224-251, 420-424).

Regarding claims 20 and 23, the combination of Hartman and Litwin does not expressly disclose using padding. However, Menezes teaches using padding with encryption (chapter 9), randomly using padding bits (page 420), **(claim 20)** placing padding of different lengths between those symbols in a ciphertext that originate from a plaintext (pages 332-334, 420-424), **(claim 23)** placing padding of different lengths at the start and/or end of a ciphertext (pages 332-334). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use

such padding methods to encrypt the plaintext information. One of ordinary skill in the art would have been motivated to do so because it was well known to use different types of padding to disguise content being exchanged between parties.

Regarding claims 22 and 25, the combination of Hartman and Litwin does not expressly disclose placing copies of symbols that occur in the plaintext as padding information. However, Menezes teaches using padding with encryption (chapter 9), randomly using padding bits (page 420) and Examiner takes Official Notice that placing copies of symbols that appear in the plaintext as padding information was conventional and well known, these symbols would be discarded by the recipient in order to decipher the ciphertext. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to place copies of symbols that occur in the plaintext as padding information between symbols and/or at the start/end of a ciphertext since Examiner takes Official Notice that it was conventional and well known.

Regarding claims 21 and 24, the combination of Hartman and Litwin does not expressly disclose placing encoded information about the encryption process as padding information. However, Menezes teaches using padding with encryption (chapter 9), randomly using padding bits (page 420) and Examiner takes Official Notice that placing encoded information regarding an encryption process as padding information was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to place encoded information regarding an encryption process as padding information between symbols

and/or at the start/end of a ciphertext since Examiner takes Official Notice that it was conventional and well known.

18. Claims 18-19, 26-27, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman and Litwin, and further in view of Schneier (NPL document "Applied Cryptography").

Regarding claim 18, the combination of Hartman and Litwin does not expressly disclose permuting the positions of all of the symbols in an input plaintext sequence, according to a given permutation, the permutation being performed over the entire length of the plaintext sequence. However, Schneier teaches transposition ciphers (pages 10-17). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to permute (transpose) the position of the symbols. One of ordinary skill in the art would have been motivated to do so because it was well known to use transposition ciphers (Schneier, pages 10-12).

Regarding claim 19, the combination of Hartman and Litwin does not expressly disclose permuting the positions of the symbols in subsequence blocks of an input plaintext sequence, according to a given permutation, the subsequence blocks not necessarily all being of the same length. However, Schneier teaches transposition ciphers (pages 10-17). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to permute (transpose) the position of the symbols using blocks of different length. One of ordinary skill in the art would have been motivated to do so because it was well known to use transposition ciphers (Schneier, pages 10-12).

Regarding claim 26, the combination of Hartman and Litwin does not expressly disclose circularly rotating the ciphertext during encryption. However, Schneier teaches rotor machines ciphers (pages 10-17). Furthermore, Hartman teaches a processor for encryption/decryption. Applicant also admits the use of padding was known (page 1). Furthermore, Examiner takes Official Notice that decrypting using a function (to decipher an encoded message) and using padding was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt using a rotor machine cipher and add padding. One of ordinary skill in the art would have been motivated to do so because it was well known to translate plaintext symbols into other plaintext symbols (Schneier, pages 10-12).

Regarding claim 27, the combination of Hartman and Litwin does not expressly disclose circularly rotating the ciphertext during decryption. However, Schneier teaches rotor machines ciphers (pages 10-17). Furthermore, Hartman teaches a processor for encryption/decryption. Applicant also admits the use of padding was known (page 1). Furthermore, Examiner takes Official Notice that decrypting using a function (to decipher an encoded message) and using padding was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt using a rotor machine cipher and add padding. One of ordinary skill in the art would have been motivated to do so because it was well known to translate plaintext symbols into other plaintext symbols (Schneier, pages 10-12).

Regarding claim 32, the combination of Hartman and Litwin does not expressly disclose in which the plaintext symbols are systematically translated into other plaintext symbols. However, Schneier teaches substitution ciphers (pages 10-17). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to systematically translate plaintext symbols into other plaintext symbols. One of ordinary skill in the art would have been motivated to do so because it was well known to translate plaintext symbols into other plaintext symbols (Schneier, pages 10-12).

Conclusion

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US Patent Number 5,541,996 to Ridenour and US Patent Number 6,732,278 to Baird, III et al. disclose using true random number generators for encryption purposes.

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

Primary Examiner
AU2131
9/23/05